UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC.,

                Plaintiff,

        v.

SKYRYSE, INC., ROBERT ALIN
PILKINGTON, MISOOK KIM, and DOES NOS.
1-50,

                Defendants.

Case No. _____

COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Moog Inc. ("Plaintiff" or "Moog"), by and through their undersigned

counsel, Sheppard, Mullin, Richter & Hampton LLP, for its Complaint, alleges against

Defendants Skyryse, Inc. ("Skyryse"), Robert Alin Pilkington ("Pilkington"), Misook Kim

("Kim"), and DOES Nos. 1-50 (collectively, "Defendants") as follows. The allegations

herein are made based on personal knowledge as to Plaintiff and its own actions and

interactions, and upon information and belief as to all other matters.

NATURE OF THE ACTION

1.   Moog seeks judicial relief to stop the illegal taking and use of its trade

secrets and the misappropriation of sensitive US Government technical data developed by

Moog. The Defendants' illegal and improper acts are predicated on: a prior business

relationship between Moog and Skyryse from 2018-2020; Skyryse suddenly changing its

business model to overlap with Moog's after the business relationship ended; Skyryse

hiring 20 of Moog's senior staff and best software engineers; and a former Moog employee

(and named Defendant herein) stealing over 136,000 files of Moog's most sensitive and

proprietary data (and government contracts related data) related to its flight control

software (including 43,960 source code files) that took over 15 years to develop by dozens of Moog engineers, just weeks before leaving Moog and joining Skyryse.

2.   The cover up is just as egregious. A forensic inspection of the external hard drive used to copy over 136,000 files of Moog's data reveals that, before its eventual return to Moog several months after the copying took place, it was intentionally wiped during a reformatting process which makes it impossible for Moog to determine which of its files were copied, accessed, or modified and what other computers or devices may have been subsequently connected to the external hard drive at issue. The inspection also confirmed that additional acts of copying Moog data took place, and Defendants deliberately deleted data and re-named devices to try to cover their tracks.

3.   This is an action for breach of contract, misappropriation of trade secrets pursuant to the federal Defend Trade Secrets Act, state and common law misappropriation, unfair competition, tortious interference with economic advantage, breach of fiduciary duty, aiding and abetting breach of fiduciary duty, conspiracy, and unjust enrichment arising out of Skyryse's and the individual defendants' egregious and ongoing acts of contractual violations, intellectual property misappropriation, corporate raiding, and interference with Moog's business.

4.   These causes of action seek to redress a coordinated scheme by Defendants to misappropriate valuable confidential, proprietary, and trade secret information by way of stealing it, and further recruit swaths of Moog's valuable employees to use that misappropriated information to improperly shortcut Skyryse's own research and development costs and timeline to give Skyryse a competitive advantage, and undercut, steal, and/or interfere with Moog's business.

5.   Both Defendants Pilkington and Kim were senior level Moog software engineers and were given access to, and were involved in the development and testing for, extremely sensitive Moog proprietary information having commercial and US Government program applications. This included, without limitation, Moog's executive Platform base flight control software and related project-specific applications, developed over many years.

6.   As a part of this scheme, Pilkington, a long-time Moog employee, left Moog in November 2021 to join Skyryse. Then, on information and belief, on behalf of and in coordination with Skyryse, Pilkington instructed Kim, while she was still an employee of Moog, to copy and misappropriate an enormous amount of Moog's confidential, proprietary, and trade secret data and program files (and government contracts related data) – 136,994 files in total -- and to provide such information to Pilkington and Skyryse for improper use. Such information, which includes the source code of highly proprietary software programs that are critical to Moog's ability to provide services to its many commercial and government customers, is the result of years of manpower and hundreds of millions of dollars invested by Moog. Defendants' improper use of this confidential and sensitive information, if not stopped will lead to irreparable harm to Moog, give a competitor an extreme and unfair advantage in a highly competitive emerging market, and severely impact both Moog's current and future business.

7.   Further, the Defendants' targeted, improper, and ongoing raiding of Moog's software engineering force, which has resulted in a loss of dozens of critical developers and engineers, presents substantial disruption and jeopardy to Moog's ongoing business. Skyryse is unfairly competing by simultaneously crippling Moog's staffing numbers while

having former Moog employees utilize and build on Moog's confidential, proprietary, and trade secret information for Skyryse's benefit.

8.   If Defendants are not stopped, they will continue to more completely integrate, utilize, and improperly trade upon decades' worth of misappropriated information belonging to Moog in an attempt to beat Moog and several other competitors in the unmanned aircraft market, and will continue to methodically and increasingly plunder Moog's employees in an effort to unfairly shortcut Skyryse's own development process. In doing so, Defendants will irreparably harm Moog.

9.   Moog seeks injunctive relief and to recover damages arising from Defendants' unlawful conduct. Defendants' conduct was and continues to be willful and malicious. Moog further seeks injunctive relief to prevent Defendants from fully consummating their scheme to take Moog's business and/or improperly augment and accelerate Skyryse's business through improper use of the misappropriated information and expanded hiring of Moog's employees for the relevant business.

THE PARTIES

10.   Founded in 1951 in East Aurora, New York, Moog is a publicly traded (NYSE: MOG.A, MOG.B) aerospace and defense company. It has annual sales of approximately $3 Billion and a world-wide workforce of over 13,000. Moog is a designer and manufacturer of electric, electro-hydraulic and hydraulic motion, controls and systems for applications in aerospace, defense, industrial and medical devices. The company operates under three segments: aircraft controls, space and defense controls, and industrial controls. Moog has developed and supplies the flight control systems for some of the most common commercial aircrafts used today, including the Boeing 787, Airbus A350, Embraer E2

regional jet and multiple business jets for Gulfstream and others. It has also developed systems and components for some of the most critical commercial and government sponsored space and defense systems, including the International Space Station, United Launch Alliance, and Apollo mission. Moog works frequently on sensitive United States government projects, as well as third-party commercial projects. Moog has sales, engineering, and manufacturing facilities in twenty-six countries. Moog is a New York corporation. Moog's corporate headquarters are located at 400 Jamison Road, East Aurora, New York.

11.   Defendant Skyryse, Inc. is a Delaware corporation with its principal place of business at 777 Aviation Blvd, El Segundo, California. Skyryse is a venture-backed tech aviation start-up company founded by CEO Mark Groden in 2016. Skyryse is privately held and Plaintiff is unaware of its annual sales. Skyryse's stated goal is to build autonomous flying aircraft, *i.e.*, aircraft without pilots, and to build such autonomous flying systems into already-developed aircraft. Skyryse had an initial venture capital funding of $25 million and announced in October 2021 another $200 million investment by various venture capital firms. Skyryse total employment is unknown to Moog, but the current employees of Skyryse hired from Moog are believed to form a significant portion of Skyryse's technical workforce.

12.   Defendant Robert Alin Pilkington is a resident of the State of California. Pilkington was employed by Moog from on or about July 30, 2012 to November 12, 2021. At the time of his resignation from Moog, Pilkington held the position of Software Manager and worked at Moog's Torrance, California facility. Pilkington's last known home address is 1281 Cabrillo Avenue, Unit 401, Torrance, California 90501.

13.   Defendant Misook Kim is a resident of the State of California. Kim was employed by Moog from on or about January 21, 2013 to December 18, 2021. At the time of her resignation from Moog, Kim held the position of Software Engineer and worked at Moog's Torrance, California facility. Kim's last known home address is 2120 Bridgeport Way, Torrance, CA 90503.

14.   The true names and capacities, whether individual, corporate, associate, or otherwise, of defendants DOES 1 through 50, inclusive, are presently unknown to Plaintiff, who therefore sues said defendants by such fictitious names and will ask leave to amend the Complaint to show their true names and capacities when they have been ascertained. Plaintiff is informed and believes and thereon alleges that each of the defendants designated herein as DOE is responsible in some manner for the events and happenings referred to in this Complaint.

15.   At all relevant times, all Defendants were agents of and acting on behalf of each other.

JURISDICTION AND VENUE

16.   This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1331 because this action arises, in part, under the Defend Trade Secrets Act, 18 U.S.C. § 1836, *et seq*. ("DTSA"). The DTSA additionally states that "[t]he district courts of the United States shall have original jurisdiction of civil actions brought under this section." 18 U.S.C. § 1836(c). This Court has jurisdiction over Plaintiff's state law claims under 28 U.S.C. § 1332 because the parties are of diverse citizenship and the amount in controversy exceeds $75,000, exclusive of interest and costs.

17.   This Court maintains supplemental jurisdiction over Moog's state and

common law claims pursuant to 28 U.S.C. § 1367.

18.   This Court has personal jurisdiction over Defendants because each of them

committed the torts alleged below within the state, and to the extent any tortious acts were

committed without the state, the acts of Defendants have caused injury to Moog within the

state. The contract claims in this case include New York choice of law provisions, and

Moog, a New York company, is a counterparty to all relevant agreements and was in New

York at the time that all agreements were negotiated and executed. The contracts also were

performed at least partially in New York.

19.   Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because, as

alleged below, a substantial part of the events giving rise to Moog's claims occurred in this

district and/or the Defendants are subject to the Court's personal jurisdiction in this district

with respect to this action.

MOOG'S FLIGHT CONTROL SOFTWARE

20.   Moog is a worldwide designer, manufacturer and integrator of precision

control components and systems. The company offers wide range of aircraft controls,

space and defense controls, industrial systems and medical devices. Moog additionally has

designing and manufacturing capabilities in motion control systems and components,

control and power electronics, software, and fiber optics.

21.   Moog designs, manufactures, and integrates precision motion and fluid

controls and systems for various applications in the aircraft, aerospace, automated

industrial machinery, marine, medical equipment, oil and gas, defense, power generation,

construction, and simulation industries, and operates a network of manufacturing facilities

in the United States, as well as in countries such as the United Kingdom, the Philippines, Germany, China, Italy, Brazil, India, the Czech Republic, Costa Rica, Luxembourg, Canada, the Netherlands, Lithuania, Ireland, and Japan.

22.   Moog designs and manufactures the most advanced motion control products for aerospace, defense, industrial and medical applications – applications where precise control of velocity, force, acceleration and fluid flow are critical. Moog's motion control portfolio includes all forms of actuation technology, sophisticated control and power electronics and system software. Moog is a leading integrator of precision motion control systems.

23.   The company's largest business segment is aircraft controls, which generates revenues from military and commercial aircraft in addition to aftermarket support.

24.   As part of its motion control product portfolio, Moog develops software that governs flight controls for airplanes and other aircrafts, including helicopters. Moog has been in the business of development, testing, and certification of flight control software and applications since at least as early as 1999.

25.   Among its many offerings, Moog develops software that "pairs up" with the hardware computers contained inside aircraft. Moog's flight control software provides utilities that the particular airplane application can use to interface with the hardware that the pilot is using in the aircraft. For example, when a pilot moves a control in the cockpit, Moog's software reads the control and moves the particular component of the airplane. Moog's flight control software also has actuation functions. In short, Moog's flight control software works in tandem with an aircraft's computer to control its flight and navigation functionality.

26.   Moog's base flight control software for commercial use is called Platform. It is the executive software that runs other flight control applications. Platform is in essence the "operating system" that an aircraft's computer uses, similar to Windows or Mac OS for a standard home computer. On top of the base operating system, applications specific to the particular aircraft involved are built and sit on top of the Platform base operating system to tailor its functionality to the particular aircraft. This is akin to downloading a program or application and running it on a Windows or Mac OS operating system on a standard computer. The particular application provides a specific use, but the underlying operating system allows the entire system and machine to work.

27.   Over the past 15 years, Moog has developed three major branches of the Platform base flight control operating system software: one for commercial aircrafts, one for military use (called "eRTOS"), and one for motor applications (called "AMP").

28.   Platform is the generic name for the first iteration used on all commercial programs. Platform is being used in many widespread and common commercial airplanes today, including aircrafts such as 747, G280, G650, and C919.

29.   Moog develops project-specific software applications for military use, which sit on top of the Platform flight control operating system, and specifically, the "eRTOS" base software.

30.

███████████████████████████████

███

31.   The base Platform software, and its military and motor iterations, allow Moog to tailor its aircraft-specific software very quickly based on the particular needs of that aircraft or project. Platform provides the base flight control software such that Moog only needs to develop an additional layer of software for the flight controls of a particular type of aircraft.

32.   Moog has invested millions of dollars in software engineering hours to develop the original Platform base software for commercial use, a sum which does not include the amount of time or money used to develop Platform's military or motors iterations, or any project-specific applications.

33.   The source code for Platform base software and related project-specific applications, as well as documentation and information regarding the development, modification, improvement and deployment of the Platform, constitute Moog's most valuable, sensitive, and proprietary information.

34.   The novel realization of an adaptable Platform software provides Moog a considerable and valuable competitive advantage in the marketplace. The uniquely-adaptable Platform allows Moog to be the front-runner in obtaining contract awards from commercial or military customers.

35.   The three iterations of the Platform base software (commercial, military, motors) took 15 years in total to develop, and building each iteration of the Platform software required 10 full-time software engineers over a period of two to three years.

36.   On top of the multiple years it took to build Platform, the testing and certification

requirements for flight control software are extremely vigorous and costly. Before any flight

control software is approved by the Federal Aviation Administration ("FAA") or similar

governing bodies around the world, it must be vigorously tested and certified. Different types of

testing and analyses are required. It takes twice as long to test and certify flight software than it

does to construct it. Testing and certification generally constitutes two-thirds of Moog's total

cost to build flight software.

37.   Moog has invested approximately ▮▮▮▮▮ in building, testing, and

certifying its Platform base software over the past 15 years, and invested approximately

▮▮▮▮▮ in building, testing, and certifying its aircraft project-specific software

applications that sit on top of the Platform software.

38.   Were a competitor to obtain and be allowed to exploit Moog's Platform base

software, or any component of it, it would provide a huge competitive advantage to that

company. If a third party had possession of Moog's Platform software, including its

underlying code, testing, and certification requirements, the third party company could

easily "click and build" a project specific software on top of the base software in a short

amount of time. The only thing the party would need to build a project-specific application

is an electronic computer from a particular aircraft to connect to.

39.   The types of information relating to Platform and related project-specific

applications that Moog always treats as internal trade secrets that are never disclosed to

other parties are: 1) the source code for these programs; and 2) certain documents and

checklists prepared by Moog's Software Engineering Process Group ("SEPG"), which

contain processes to ensure that the software is being developed in a manner to meet

certification requirements by the FAA and other similar authorities around the world. The SEPG documents have been optimized over 20 years of working with aviation authorities around the world. Many companies hire Moog for software development specifically because Moog knows how to efficiently create and certify software with the world's various aviation authorities.

MOOG'S MEASURES TO PROTECT ITS INTELLECTUAL PROPERTY

40.   Given the confidential and valuable nature of Moog's software, including Platform, Moog takes the security of its software very seriously, and employs several important security measures to control and limit access to the software and protect against theft or misuse thereof.

41.   Moog employees are required to sign Moog internal proprietary information agreements, as well as third party proprietary information agreements when working on certain project-specific applications, including sensitive government projects.

42.   Moog also requires its departing employees to sign an exit form wherein each individual confirms they have been provided access to Moog's proprietary and trade secret information, have returned all Moog IP upon departure, and have not maintained access to or copies of any digital record of Moog's.

43.   Further, Platform, including all attendant project-specific software, is housed on a secure server at Moog and only certain employees at Moog have access to the software database. Access to the software database is on a "need to know" basis that must be approved by the lead on the software program. For example, an employee can work on a software program but not be given access to the software database if the program lead determines that employee does not

require access to the software database. In order to have access to Platform and related project-specific software, a Moog employee would need five separate credentials.

44.   Moreover, the Platform software as applied to military projects is extremely sensitive to the US Government. Only a limited number of individuals have the necessary access credentials to work on the Sensitive Government Programs. To obtain such access credentials is time consuming and requires extensive vetting.

45.   Under its government contracts, Moog is obliged to implement extensive security measures to safeguard and protect sensitive information. These security measures include, *inter alia*, access restrictions, authentication, encryption, physical protections, and specific training for employees. Moog also adheres to additional requirements and protections for sensitive data for certain of its government customers.

46.   Further, the Platform software itself is designed to prevent hacking or reverse engineering. It cannot be reverse engineered from an aircraft computer that has used the software.

47.   With respect to its facilities, Moog has controlled access into its buildings, and all employees must undergo security screening and a background check before being hired.

48.   Every new Moog hire (including any software engineer) is required to review the then-current Moog employee handbook and acknowledge the requirements therein in writing, either through a signed paper form or an electronic acknowledgment. Pilkington acknowledged receipt and agreed to abide by Moog's employee handbook in writing on July 30, 2012. Kim acknowledged receipt and agreed to abide by Moog's employee handbook in writing on January 21, 2013. A true and correct copy of the acknowledgments signed by Pilkington and Kim are attached hereto as **Exhibit A**. A true and correct copy of

the Moog employee handbook in effect when these acknowledgments were signed (the

"Employee Handbook") is attached hereto as **Exhibit B**. The Employee Handbook

provides that Moog employees will receive access to confidential and proprietary

information, and that disclosure to any outside party is prohibited, including after

employment has been terminated. It also emphasizes that Moog employees may not retain

any copies of Moog's confidential and proprietary information.

49.   Moog also has a robust written policy governing its intellectual property,

including its internal proprietary, confidential, and trade secret information. This written

policy is made available to every Moog employee, including all software engineers. This

written policy, among other things, defines Moog's proprietary and trade secret

information, provides strict protocols for storing, designating, and transmitting such

information, and prevents any third party disclosure of such information. Moog requires its

employees (including all software engineers) to attend a training on Moog's proprietary

and trade secret information, which summarizes the contents of Moog's written IP policy.

Pilkington completed Moog's trade secrets training in July 2012 and again in October

2016, and Kim completed the training in February 2013 and again in January 2015.

50.   Every Moog flight software source code file contains a restrictive language

such as: "*MOOG PROPRIETARY and CONFIDENTIAL INFORMATION; This technical*

Data/Drawing/Document contains information that is proprietary to, and is the express

property of Moog Inc., or Moog Inc. subsidiaries except as expressly granted by contract

or by operation of law and is restricted to use by only Moog employees and other persons

authorized in writing by Moog or as expressly granted by contract or by operation of law.

No portion of this Data/Drawing/Document shall be reproduced or disclosed or copied or

furnished in whole or in part to others or used by others for any purpose whatsoever except as specifically authorized in writing by Moog Inc. or Moog Inc. subsidiary."

MOOG TEAM WORKING ON PLATFORM

51.   Gonzalo Rey (former Director of Engineering and Chief Technology Officer) and Sathyanarayana Achar (former Engineering Technical Fellow) were the first two Moog employees to sponsor and oversee the development of Moog Platform base software beginning in 2007. They have the most institutional and technical knowledge regarding the software, as well as its relationship with project-specific applications which sit on top of the base software. They are now employed by Skyryse.

52.   Michael Hunter and Todd Schmidt are two senior level engineers who have worked on and managed the programs that created Platform, and its related project-specific applications, since 2007. Both have been solicited for employment by Skyryse.

53.   Defendant Robert Alin Pilkington (former Senior Staff Engineer) was the lead architect (software engineer) on the second iteration of the Platform base software for military purposes, eRTOS. At Moog, Pilkington and his team built eRTOS beginning in 2013. As of 2016, Pilkington reported directly to Hunter. In November 2021 and at the time of his departure from Moog, Pilkington and his team were working on military project Sensitive Government Program 2, which sits on top of the eRTOS base software. They all had heightened access credentials to work on this project.

54.   One of the individuals working under Pilkington was Defendant Misook Kim, a Senior Staff Engineer. Kim had worked under Pilkington's supervision for several years. While at Moog, Kim was extremely loyal and obedient to Pilkington and routinely demonstrated that she was willing to perform any task that Pilkington needed or asked of her.

55.   As of the Fall of 2021, Moog had twenty-nine (29) software developers/engineers in the Buffalo, New York area and twenty-two (22) in the Los Angeles, California area working on the Platform software and related project-specific applications.

AS SKYRYSE MAKES PROMISE AFTER PROMISE TO INVESTORS, IT GOES TO MOOG TO TRY AND SATISFY THOSE PROMISES

56.   Moog has an Aircraft Group and an Innovation and Technology Group, which has its own subgroup for Growth and Innovation. The purpose of the Growth and Innovation Group is to explore new and innovative business opportunities for Moog outside of its existing business channels. The focus of the Growth and Innovation Group evolved over time, but gradually became more centered on flight controls and the front end of aircraft functionality. Going into 2019, the group's focus was geared more towards helicopter flight control.

57.   In 2018, Moog's Growth and Innovation Group began exploring a potential business opportunity with Defendant Skyryse, which at that point was a very new company, having just been formed in 2016 by Mark Groden.

58.   In a situation akin to Theranos, Mr. Groden was 26 years old at the time of the company's founding. He was described in the press as a "wunderkind[]…who at age 15 built an unmanned fixed-wing VTOL that was used by the U.S. military." His Forbes profile states that when he "was 16, he joined the U.S. Air Force lab at Case Western, where he built an unmanned aerial vehicle."

59.   Moog and Skyryse engaged in a series of discussions and meetings during mid-2018, in which Skyryse explained its business plan.

60.   Based on Skyryse's explanations about its business plan, Moog believed there was real potential for opportunity based on Moog's then-existing capabilities and
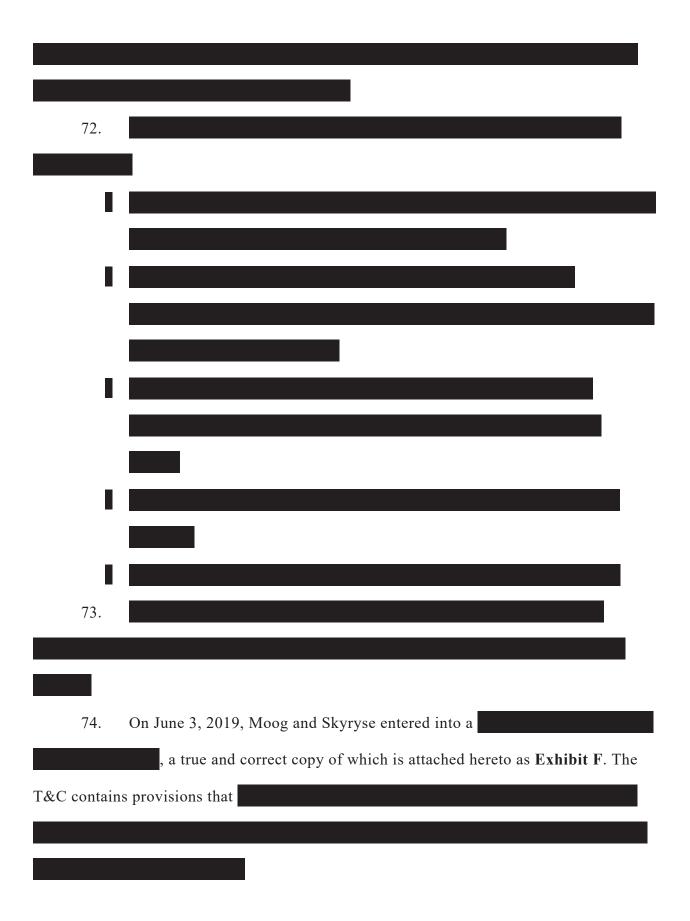
desire to enter into new markets. During these initial discussions in mid-2018, Skyryse

represented that it wanted to offer on-demand helicopter transportation to the general

public, through the use of automated flight system technology. Under this potential

structure, Moog would provide the helicopter flight control systems (including flight

control software, actuators, and computers), and Skyryse would install and implement this

technology into their business. Skyryse would have its own central computers which

would send a command to Moog about where a certain helicopter would fly to, and Moog

would take care of the flight control aspect (including takeoff, navigation, and landing).

62.   Skyryse further indicated that it wanted to own the Supplemental Type

Certification ("STC") for the unmanned, automated flight system for the R-44 helicopters.

62.   Any type of software, hardware, or other technology that goes into a

helicopter requires a STC issued by the FAA. This means that the FAA has authorized the

certain technology or software to go into the helicopter. Because Skyryse wanted to own

the STC for this technology, Moog demanded (and Skyryse agreed) that Skyryse would

perform and take responsibility for all installation of Moog's technology into Skyryse's R-

44 helicopters.

63.   Under Skyryse's initial proposed business model, Skyryse's goal was to

eventually offer unmanned helicopters through an automated flight system. However, in

the early stages of its business Skyryse intended to have a safety pilot on board that could

override the automated flight system and take control if needed.

64.   As these business discussions progressed and to facilitate an exchange of

information to evaluate a potential business opportunity, on October 24, 2018, Moog and

Skyryse entered into a "Proprietary Information and Nondisclosure Agreement" (the "2018

NDA"), a true and correct copy of which is attached hereto as **Exhibit C**. The 2018 NDA's express scope was for the "[e]xchange of business and technical information in various forms and forums."

65.   At the time of the initial NDA, Skyryse had closed $25 million in seed and Series A funding – on or around August 28, 2018. In press articles in connection with the funding, Skyryse was described as having "aspirations to work on technology for FAA-approved vertical take-off and landing (VTOL) aircraft."

66.   As discussions continued to progress, on March 15, 2019, Moog and Skyryse entered into another "Proprietary Information and Nondisclosure Agreement" (the "2019 NDA"), a true and correct copy of which is attached hereto as **Exhibit D**. The 2019 NDA contains the same material terms as the 2018 NDA. However, the 2019 NDA's express scope was for: "Discussion of integration of Moog's flight control systems /subsystems / components and associated autonomous control technologies with Skyryse's aircraft platforms and associated autonomous control technologies."

67.   Under these NDAs, the Parties agreed not to disclose any proprietary information disclosed by the other parties, and the receiving party of such information could only use it for the limited purpose of the contemplated engagement between Moog and Skyryse. (*Id*. at § 2). The NDAs both had an effective term of 10 years. (*Id*. at § 5). The Parties agreed that any breach of the NDAs would result in "irreparable and continuing damage" and that the "non-breaching Party shall be entitled to seek injunctive relief, without the necessity of posting a bond." (*Id*. at § 8). Both the 2018 NDA and 2019 NDA also contained New York choice of law provisions. Moog performed substantial services and deliverables under both the 2018 and 2019 NDAs out of its New York headquarters.

68.   Moog and Skyryse's business relationship was contemplated to be conducted in four separate phases, with the Parties agreeing to enter into a separate contract before each phase. On May 31, 2019, Moog and Skyryse entered into a ████████████████ ███████████████████████████████████ (hereafter, the "SOW"), a true and correct copy of which is attached hereto as **Exhibit E**.

69.   ██

██

███

███████████████████████████████████████

████████████████████████████████████

███

██

70.   ██████████████████████████████████████

███

█████████████████████████████████

  ▌ ███████████████████████████████

  ▌ █████████████████████████████████████

  ▌ ███████████████

  ▌ █████████████████████████████████████

     ████████████████████████████

71.   ██

██

██

████████████████████████████████

72.   ███

███████████████

  ▌   ██

      █████████████████████████████████████

  ▌   ██

      ██

      ███████████████████████████

  ▌   ███

      ██

      ███████

  ▌   ██

      ██████████

  ▌   ██

73.   ██

██

███████

74.   On June 3, 2019, Moog and Skyryse entered into a ████████████████

██████████████, a true and correct copy of which is attached hereto as **Exhibit F**. The

T&C contains provisions that ███

███

███████████████████████████

75.   Moog met its obligations under the SOW, specifically ███████████

███

███████████████████████████████

76.   Before the parties were to explore Phase 2, Skyryse intended to take its

system live to the public. On information and belief, Skyryse's launch did not go as

planned and was not successful. By October of 2019, Skyryse stopped its business

operations, fired many of its employees, and was looking to pivot its business model.

77.   On December 17, 2019, Skyryse issued a press release proclaiming that it

was offering an autonomous flight system as part of a flight control operating system. It

called the automation technology "Flight Stack". On the same date, it revealed that it had

obtained another $13 million in financing.

78.   Skyryse additionally revealed "Luna," which was very similar to Moog's

name for its autonomous flight system previously discussed with Skyryse, "Lucy." "Luna"

was described at the time as "a Robinson R44 helicopter retrofitted with the company's

autonomy technology."

79.   Skyryse had pivoted into exactly what Moog was doing, and the previously

separated and defined roles for Moog and Skyryse became blurred.

80.   Skyryse next announced the launch of what it called "FlightOS" on March

17, 2020. Skyryse's press release described FlightOS as "combining on-board computers and

fail-operational flight control automation hardware to power a new class of envelope protection

and emergency management. The system constantly monitors the aircraft's movement, stability,

and flight path to ensure flight operations remain within all aspects of the flight envelope

capabilities." It also proclaimed that with FlightOS, "on-board computers control all aspects of

the flight envelope, manage the airframe's structural and aerodynamic operating limits, and leverage exterior radar and sensors for real-time situational awareness."

81.   Skyryse also took a dig at Moog, proclaiming "[f]or decades, there has been little technological advancement in general aviation."

82.   Notwithstanding these proclamations, on May 22, 2020, Skyryse issued a request for quote ("RFQ") to Moog, a true and correct copy of which is attached hereto as **Exhibit G**. The RFQ was sent by Tim Baptist of Skyryse, who was formerly Aircraft Group Vice President at Moog before leaving in February 2020. In the RFQ, Skyryse stated that it was "ramping up the second phase of the go-to-market program with the certification FlightOS on a light helicopter." The RFQ also states that Skyryse's "goal is to certify a system with a simplified pilot interface that makes flying safe and easy to learn for a broad cross-section of the public." Moog's deliverables under the RFQ would consist of the following:

- Develop a single triple redundant actuator version of the dual redundant one developed over the past year with Skyryse

- Re-package an existing computer to incorporate all flight sensors, battery and charger into a triple-dissimilar redundant set as described in the SOW

- Develop a side stick as described in the SOW

- Deliver a lab system (Blue Label) in January of 2021

- Deliver a flight test system (Red Label) in July of 2021

- Certification baseline system (Black Label) in December 2021

83.   In short, Skyryse requested that Moog provide flight control computers and actuator systems for Skyryse to use and to implement Skyryse's flight control operating

system software. Providing flight control computers and actuator systems for aircrafts was already an established line of business for Moog. So, Moog, focused on innovative and new business opportunities, was reluctant to pursue that line of business with Skyryse, especially since Skyryse had changed its entire business plan and model compared to when Moog first started doing business with Skyryse.

84.   Nonetheless, given the prior business relationship with Skyryse, and the fact that several former respected Moog employees worked at Skyryse, on September 22, 2020, Moog submitted a bid in response to Skyryse's RFQ for $46,195,870, a true and correct copy of which is attached hereto as **Exhibit H**.

85.   Shortly after Moog submitted its bid, Skyryse notified Moog that Moog's proposal was too expensive and Skyryse would be going elsewhere.

86.   After it was evident that Moog and Skyryse would not pursue any further business opportunity, there was additional correspondence between the companies about closing up Phase 1. The Parties did not pursue any further business opportunities. Phase 1 concluded, but the terms of the 2018 and 2019 NDAs were never terminated.

87.   It was therefore surprising, to say the least, when on October 27, 2021, Skyryse announced a $200 million Series B fundraise in support of its FlightOS product. In the press release, Skyryse's CEO, Mark Groden, proclaimed in the press release that "[t]he general aviation industry is about to change forever."

SKYRYSE'S POACHING OF MOOG EMPLOYEES

88.   Notwithstanding the image it presents in its press releases, Skyryse is in the process of pursuing unmanned helicopter aviation in a highly competitive emerging market, one

in which approximately twenty (20) companies are racing to become the industry leader by releasing successful, safety-tested, certified, and comprehensive unmanned aviation systems.

89.   Facing considerable pressure to meet investor expectations and obtain a significant advantage against competitors, Skyryse made the strategic decision to take what it could not develop quickly enough, and engage in a "full court press" to take from Moog as many key employees as possible so that it can shortcut its own timeline and costs in developing automated flight software and related products.

90.   In recent months, in order to unfairly compete, Skyryse has engaged in a methodical, intentional, and pervasive raid of Moog's developers who built Platform and resulting project-specific applications. Indeed, the majority of such developers have been poached by Skyryse, with most of these departures occurring in the past few months. And as a result, many of the primary individuals involved in the development, testing, and certification of Platform now work at Skyryse.

91.   The following is a list of current and former Moog employees who have joined Skyryse or have notified Moog that they will be leaving Moog to join Skyryse (as well as showing reason for departure, final day at Moog, position, and location):

- o Gonzalo Rey – Voluntary termination 8/1/2017; Role: Chief Technology Officer; Location: East Aurora, New York
- o Tony Chirico: Retired 9/28/2019; Role: Senior Staff Engineer; Location: East Aurora, New York
- o Tim Baptist – Retired 2/29/2020; Role: Group Vice President; Location: Torrance, California
- o Robert Alin Pilkington – Voluntary termination 11/12/2021; Role: Sr. Staff Engineer; Location: Torrance, California
- o Sathyanarayana Achar: Retired 1/2/2022, Role: Engineering Technical Fellow; Location: Torrance, California
- o Nigel Cranwell: Retired 11/1/2021, Role: Electronic Operations Manager; Location: East Aurora, New York
- o Eric Chung – Voluntary termination 12/3/2021; Role: Sr. Staff Engineer; Location: Torrance, California

- o Misook Kim – Voluntary termination 12/17/2021; Role: Sr. Staff Engineer; Location: Torrance, California
- o Lawrence Chow – Voluntary termination 12/17/2021; Role: Software Design Engineer; Location: Torrance, California
- o Reid Raithel – Voluntary termination 1/7/2022; Role: PE/NPI Sr. TE Engineering Manager; Location: Torrance, California
- o Victor Nicholas – Retired 1/21/2022; Role: Supply Chain Manager; Location: Torrance, California
- o Mario Brenes – Voluntary termination 2/5/2022; Role: Software Engineer; Location: Torrance, California
- o Cynthia Le – Voluntary termination 2/10/22; Role: Software Engineer; Location: Torrance, California
- o Tri Dao – Voluntary termination 2/10/22; Role: Senior Laboratory Engineer; Location: Torrance, California
- o Santiago Correa-Mejia – Voluntary termination 2/18/22; Role: Development Engineer; Location: Torrance, California
- o Chi Hsin Alex Wang – Voluntary termination 2/20/22; Role: Test Equipment Section Head; Location: Torrance, California
- o John Stafford – Voluntary termination 2/25/22; Role: Associate Engineer; Location: Torrance, California
- o Alan Lee – Voluntary termination 2/28/22; Role: Development Engineer; Location: Torrance, California
- o Dan Gunderson – Voluntary termination 3/4/22; Role: Design Engineer Location: Torrance, California
- o Paul Kapuan – Planned voluntary termination to be effective 3/31/22; Role: E1 Sr. Staff Engineer; Location: East Aurora, New York

92.   Certain key, senior individuals such as Gonzalo Rey, Sathyanarayana Achar, and Pilkington are extremely familiar with and knowledgeable regarding Moog's Platform base software and related project-specific applications, as well as the more capable members of Moog's software engineering teams who worked on these programs.

93.   Additionally, several of these individuals hold extremely senior positions within Skyryse where they are in a position to drive the company's strategy and decision making. Tim Baptist, who was formerly a Moog group vice president, is currently Skyryse's Chief Operating Officer (COO). Gonzalo Rey, who was Moog's Chief Technology Officer (CTO), is currently Skyryse's CTO and sits on Skyryse's Board of Directors.

94.   Rey, Pilkington and other Skyryse employees, in a strategic effort to carry out Skyryse's raid of Moog, systematically worked to recruit Moog employees to join Skyryse.   For example, in August 2021, Gonzalo Rey attempted to lure Michael Hunter to Skyryse, although Mr. Hunter did not pursue the conversation.

95.   For and on behalf of Skyryse, Gonzalo Rey also attempted to poach other Moog employees. For example, Rey also attempted to recruit Todd Schmidt, who resides and works in New York for Moog, to work for Skyryse.

96.   On October 13, 2021, Mr. Rey reached out to Todd Schmidt via text message to see if Mr. Schmidt had interest in joining Skyryse. The two spoke on the phone the following day. During the phone call, Mr. Rey walked Mr. Schmidt through what Skyryse was doing, plans for where Skyryse wanted to go, and advised Mr. Schmidt that he would like Mr. Schmidt to join Skyryse.

97.   Specifically, Mr. Rey told Mr. Schmidt that Skyryse's goal was extracting flight control functions to an iPad type of interface, the goal being that anyone who can use an iPad can fly a helicopter. Mr. Rey also told Mr. Schmidt that Skyryse wanted to provide an entire system that could fly an aircraft, including software, actuator functions, flight controls, computer hardware, etc. Mr. Rey communicated that Skyryse's grand vision was taking that simplified iPad type of interface to any aircraft—therefore, at some point in the future, any lay person could fly any aircraft using that simplified interface. Mr. Rey told Mr. Schmidt Skyryse's goal was to have a functional product released to the public "within a couple years" and that Skyryse had big investors coming on board to help fund the company's goals. Mr. Rey made it clear to Mr. Schmidt that Skyryse was pursuing all flight control components—software, hardware, and actuation. Thus, it was evident that

Skyryse was trying to swiftly re-produce the types of products that Moog had been developing over the course of decades.

98.   In connection with the job offer to join Skyryse, Mr. Rey advised that he was looking for a four-year commitment from Mr. Schmidt. He advised Mr. Schmidt that he needed Mr. Schmidt and others to navigate "technical challenges" at Skyryse and to help with FAA certification issues. Mr. Rey told Mr. Schmidt that he wanted Mr. Schmidt to lead Skyryse's engineering team. While Mr. Rey did not make a specific monetary offer to Mr. Schmidt, he said something to the effect of: "You would become very wealthy." At the conclusion of the telephone conversation, Mr. Schmidt told Mr. Rey that he would consider and get back to him.

99.   All of these communications occurred while Mr. Schmidt was in New York.

100.   On October 27, 2021, Mr. Schmidt texted Mr. Rey advising that he was not interested in joining Skyryse for various reasons. Mr. Rey replied and asked if Mr. Schmidt was interested in working remotely, and described other scenarios where Skyryse allowed it staff to work remotely full-time. Mr. Schmidt advised Mr. Rey that he was not interested in joining Skyryse.

101.   Pilkington resigned from Moog on November 11, 2021.

102.   Once at Skyryse, Pilkington also reached out to Mr. Hunter in or around November 2021 and asked Mr. Hunter to join Skyryse. Mr. Hunter resides in and works in New York for Moog. Pilkington later told Mr. Hunter there was "urgency" at Skyryse. Mr. Hunter declined Mr. Pilkington's offer. Mr. Hunter was in New York when this phone call occurred.

103.   On November 15, 2021, Deb Morisie (Head of People at Skyryse) called Moog's

Software Chief Engineer Jorge Lopez and offered him a job at Skyryse. Later that day, Ms.

Morisie texted Mr. Lopez asking to set up a further call. On November 17, 2021, Mr. Lopez

advised Ms. Morisie via text that he would not be pursuing a potential job opportunity at

Skyryse.

104.   Kim left Moog to join Skyryse on or about December 18, 2021.

105.   Upon information and belief, Skyryse has reached out to a large number of

software engineers at Moog who worked on the Platform software or related project-

specific applications in the United States, primarily targeted at Moog's Los Angeles-area

office.

106.   To date, Skyryse has hired twenty (20) former Moog employees, and the list

is expanding on a weekly basis. All of these former Moog software employees had

substantial and direct involvement in the building, testing, and certification of Moog's

Platform flight control software as well as project-specific applications. For example, in

Moog's Los Angeles-area office, there were nine (9) developers who could write software

code. Five (5) out of these nine (9) developers have left Moog to join Skyryse.

107.   Additionally, every single software developer who worked on the military

portion of Platform software, eRTOS, has been hired by Skyryse.

MISAPPROPRIATION OF MOOG'S PROPRIETARY AND TRADE SECRET INFORMATION

108.   Suspecting that Skyryse was engaged in an all-out raid of its flight software

employees based on an increasing level of resignations and departures to Skyryse, in late January

2022, Moog had its Security Operations team look into whether individuals who had left Moog

for Skyryse, or were soon leaving Moog to join Skyryse, had taken or copied any Moog data

before their departure.

109.   As explained elsewhere herein, misappropriating Moog's developed proprietary

and trade secret information would provide to Skyryse significant competitive advantages.

110.   Moog's Security Operations team conducted an investigation into the user

accounts and data activity associated with former employees at Moog who had recently departed

Moog to begin working for Skyryse.

111.   Using those employees' user names and an endpoint policy enforcement

solution software product, Moog investigated which files had been downloaded or copied

from Moog's internal servers onto removable devices (i.e., external hard drives, USB

devices, etc.).

112.   Moog's security investigation revealed that, while still a Moog employee, on

November 19, 2021, Kim copied significant volume of data from Moog's internal servers to an

external hard drive, amounting to greater than 136,000 files, less than one month before her

last day at Moog, and less than one week after Pilkington, her supervisor, left Moog for Skyryse

on November 12. All of the data copied by Kim is located on Moog's central servers in East

Aurora, New York.

113.   The data Moog was able to gather from Kim's electronic devices and Moog

user profile include: (1) timestamps of when she used her removable devices; (2) the

identifying credentials and specification of the devices that were used in the data copying;

(3) the names and types of the data files that were copied over; and (4) the directory

structure and file path used in connection with the copying.

114.   The timestamps for Kim's user account show that the unauthorized copying

of Moog internal server data to the external hard drive was conducted via Virtual Private

Network ("VPN") on Friday, November 19, 2021 between 3:16 a.m. and 7:33 a.m. local

time in California. Kim's normal working hours on weekdays were 8:00 a.m. to 5:00 p.m.

in Moog's Torrance, California offices. Because the download occurred via VPN, upon

information and belief, Kim downloaded Moog's data from her home or other remote

location. Further, the time of day when Kim copied Moog's data made it easier for her to

escape detection.

115.   Moog investigated the data that was copied by Kim, and prepared a file log for the

copied data (the "File Log"), which showed that Kim copied at total of 136,994 files, consisting

of:

- 43,960 source code files;

- 5,377 spreadsheets;

- 2,831 document files;

- 954 executable files;

- 9,003 image files;

- 2,010 MAP files;

- 7,898 model files;

- 1,026 object files;

- 4,613 plain text files;

- 404 presentation files;

- 20,655 miscellaneous files; and

- 38,263 SVN logs.

116.   The data copied by Kim includes nearly all of the source code, documentation,

and related information regarding the composition, testing, and certification of Platform and

project-specific applications.

117.   Moog's review of the File Log showed that the following program

classifications were found (showing which program data and code had been copied by Kim):

118.   Moog's review of the File Log confirmed that the entire application layer for

Platform was copied by Kim, meaning that 100% of the base Platform software and its code

were copied.

119.   All three iterations (commercial, military, motors) of Platform were copied, as

well as test artifacts related to some of the iterations.

120.   In addition to the Platform base software, the data and code for several project-

specific applications were also copied, as reflected above. This includes several military

programs. Kim copied all 76 of Moog's SEPG checklists as well as other documents from its

SEPG repository. Kim essentially copied almost the entirety of Moog's flight control software engineering development efforts over the past 15 years.

121.   Each employee working on the Platform project had their own "branch" or location on Moog's server, where they could store sensitive materials they needed access to as part of their work.

122.   Moog's investigation of the File Log shows that Kim used Pilkington's branch to copy the data onto the external hard drive. As detailed below, there was no reason for Kim to access the data in this fashion, let alone copy it, aside from being directed to do so by Pilkington and Skyryse ahead of her resignation from Moog. This was not accidental, or merely incidental to some legitimate work activity for Moog.

123.   Indeed, the file path used by Kim to copy Moog's data was: "D:\Misook\ENG_Alin_Branch\Software . . . ." The file path thus shows that Kim went into Pilkington's branch and copied everything that Pilkington worked on under that branch, as well as substantial additional materials that both Kim and Pilkington had access to during their employment at Moog.

124.   Importantly, while Kim had credentials to use her own file path, on which much of the same data was stored including the Platform base software, she instead used Pilkington's file path. On information and belief, this is because she was guided and/or assisted by Pilkington in identifying what files to download. Pilkington would have had intimate knowledge of what files were stored on his file path.

125.   Kim copied the data onto an external hard drive which was issued to her by Moog, and she did not return it upon her departure from Moog. As described further below, the

hard drive was only returned later to Moog several months later after demand by Moog for its return, and the hard drive was completely wiped clean.

NO LEGITIMATE PURPOSE FOR KIM'S DATA COPYING

126.   Kim signed an exit form (the "Exit Form") on her last day at Moog, December 17, 2021, a true and correct copy of which is attached hereto as **Exhibit I**. Therein, Kim affirmed in writing that she had returned all Moog "TRADE SECRET/COMPANY CONFIDENTIAL INFO." The Exit Form also states that: 1) Kim was "provided access to [Moog's] proprietary information"; 2) she "owes a fiduciary duty to Moog to not usurp any such corporate opportunity for [her] own benefit"; 3) "use of proprietary information of Moog by [Kim] . . . would be pursued by Moog using all available means;" 4) Kim affirms that she does "not maintain access to, or have possession of, any tangible or digital record of Moog IP-whether in hard copy or digital form—on any device, cloud, or digital storage facilities." Clearly, Kim did not abide by her contractual obligations on many accounts.

127.   Exit form aside, the standard way in which Moog employees worked on Platform-related projects would have been to connect to the Moog server via virtual private network ("VPN") and access data that way. All of the data copied by Kim is located on Moog's internal servers. Even if Kim was working on a different Moog computer, she could have easily accessed all the data she copied from Moog's Subversion network using her own login credentials and branch. Even if downloading data was necessary (which it was not), a copy of the data would be stored to the user's hard drive on their Moog laptop computer – not an external hard drive.

128.   Further, at the time of her departure in December 2021, Kim was working solely on "Sensitive Government Program 2." Kim was a software testing engineer, not a code-writer. Thus, even if Kim wanted to copy certain Moog data for legitimate business purposes, she would

only have a need to copy certain verification and testing data related to Sensitive Government Program 2 (instead of the entire application layer for several projects she never touched). To support legitimate business purposes, Kim would have needed, at most, to access 0.5% of the total data that she copied on November 19, 2021.

129.   What Kim did is entirely without precedent at Moog. Moog is aware of no other instance where a Moog employee copied to an external hard drive even a fraction of the data that Kim did in November 2021.

KIM, MONTHS LATER, RETURNS TWO HARD DRIVES WHICH ARE BOTH WIPED CLEAN

130.   On January 28, 2022, Moog requested that Kim return the company-issued external hard drive she had in her possession. On January 31, 2022, Kim's sister who also works at Moog returned on Kim's behalf a hard drive to Moog. However, an initial inspection of this device, a Western Digital My Passport drive (the "Western Digital Hard Drive"), revealed it was not the external hard drive device Kim had used to copy Moog's data on November 19, 2021, *and* it had been completely wiped clean.

131.   On February 18, 2022, Moog sent a further letter to Kim demanding that she return the external hard drive in question. In response, Kim called Moog's HR employee Jamie Daly, and stated she had possession of the Moog external hard drive, had used it to download a large set of files purportedly to help other Moog employees after her departure, and that she had erased all the files from the drive. This explanation made no sense. Kim had no reason to take the unprecedented step of downloading nearly 137,000 files, the vast majority of which she had never worked on and had no use for at any time in her employment at Moog, let alone the final few weeks. No other employees indicated that they would need to continue working with Kim or needed her to maintain possession of the

utmost secure and sensitive data after her time at Moog, let alone while working for competitor Skyryse. Nor would her job duties as an engineering tester have reasonably led to her needing to reference or transmit any of this data in the course of her transition out of Moog. And, Kim signed the Exit Form where she affirmed that she had returned all confidential data to Moog and would not retain any copies.

132.   When Kim eventually returned the second hard drive, a SAMSUNG PSSD T7 SCSI Disk Device, (the "Samsung Hard Drive") to Moog on February 21, 2022, an initial inspection confirmed it had been wiped before being returned. An official forensic inspection revealed much worse.

FORENSIC ANALYSIS OF KIM'S EXTERNAL HARD DRIVES AND LAPTOP DEVICES REVEALS DELIBERATE DATA WIPING AND ADDITIONAL THEFT

133.   Bruce W. Pixley, an expert computer forensic examiner with more than 20 years of experience, performed an official forensic analysis of true and correct bit-for-bit copies of the Western Digital and Samsung Hard Drives returned by Kim, as well as her two Moog-issued laptop devices ("Dell Laptop 1" and "Dell Laptop 2"). He also reviewed the File Log.

134.   First, Mr. Pixley's analysis confirmed that Kim had indeed copied 136,994 files of Moog's data on November 19, 2021 between the hours of 3:34 a.m. to 7:33 a.m. PST from Dell Laptop 1 to the Samsung Hard Drive. When Kim copied these files, they were copied to a sub-folder on the Samsung Hard Drive called "Misook."

135.   Second, Mr. Pixley's analysis revealed that "Misook" folder on the same Samsung Hard Drive was intact when it was connected to Dell Laptop 2 on December 15, 2021. On this same date, a new folder was added to the Samsung Hard Drive called "OneNote Notebooks." Microsoft OneNote is a program that is used to store user's notes,

drawings, and screen shots. In searching Dell Laptop 2, Mr. Pixley discovered that a folder

called "OneNote Notebooks" had been stored in Kim's Documents folder, containing over

200 digital notebook files. However, on December 17, 2021, Kim's last day at Moog, the

entire "Misook" folder on Dell Laptop 2 was deleted in its entirety. The deleted "Misook"

folder contained approximately 54 GB of data. Mr. Pixley's analysis reveals that this was

an intentional user deletion of data and the data was not transferred to the user's Recycle

Bin folder where it could be easily recovered.

136.   The OneNote files contained Kim's work books created over her years of

employment at Moog, and include information helpful to her in utilizing the improperly

downloaded data files she took.

137.   Third, and perhaps most importantly, Mr. Pixley's analysis reveals that the

Samsung Hard Drive (which was used to copy 136,994 files on November 19, 2021 and

additional notebook data on December 15, 2021) was intentionally formatted sometime

after Kim's departure from Moog on December 17, 2021 and before it was returned on

February 21, 2022. When a hard drive is formatted, it needs to be connected to a computer.

Mr. Pixley determined that at the start of the formatting process, an option was used that

forced the formatting process to overwrite all sectors on the drive with zeroes. Therefore,

not only was this formatting of the Samsung Hard Drive an intentional act, but this specific

formatting process effectively wiped all previous data on the drive so it would be

unrecoverable. This formatting prevents any ability to see the data that was erased on the

Samsung Hard Drive. It also prevents any ability to determine whether, when, how, or to

where any of the underlying data on the Samsung Hard Drive was copied, transferred, or

otherwise exported to another device.

138.   Fourth, Mr. Pixley determined that the Samsung Hard Drive had a volume name of "Misook-T7." The volume name for the Western Digital Hard Drive (the initial false hard drive was returned to Moog) had been intentionally changed from its factory default name to "Misook T7," in an apparent attempt to resemble the Samsung Hard Drive that was actually used to copy Moog's data on November 19, 2021 and December 15, 2021.

139.   Mr. Pixley's analysis also revealed that that a *third* external hard drive, which has not been located or returned to Moog, was connected to one of Kim's laptops several times in late November 2021. There is no telling what Moog data exists on this third hard drive due to Kim's deliberate attempts to cover her tracks.

140.   Finally, an inspection of Kim's two Moog-issued laptop devices indicates that the back covers of the laptops have been removed because the screws were not "factory tight". The laptops' hard drives can be easily accessed and removed by removing the back cover of the laptops.

141.   In short, upon information and belief, Kim, in concert with Defendants, stole large volumes of Moog's confidential and proprietary data on multiple occasions, used a number of devices and re-named them to avoid detection, and deliberately formatted and deleted the data such that Moog cannot follow the trail of what happened to its stolen data. This conduct speaks for itself, and the investigation remains ongoing, including regarding suspicious data downloads by other employees who have left Moog for Skyryse.

THE DEFENDANTS' ACTION HAVE CAUSED AND CONTINUE TO CAUSE IRREPARABLE HARM TO MOOG

142.   Defendants' intentional and sweeping misappropriation of Moog's confidential, proprietary, and trade secret information and raid of Moog's software developer employee team have caused, and continue to cause, substantial and irreparable harm to Moog.
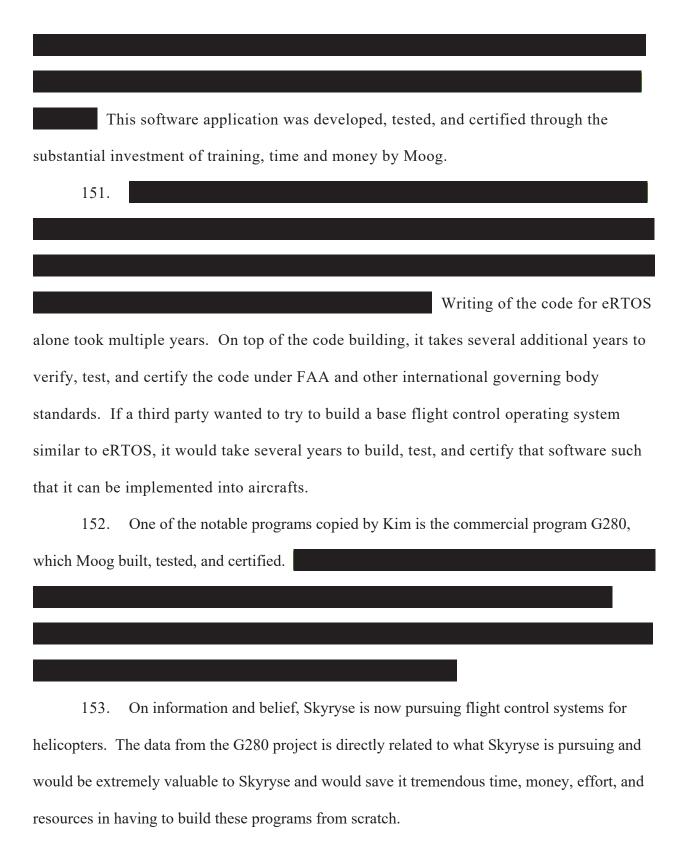
143.   Unmanned helicopter aviation, which Moog is pursuing and understands Skyryse is also pursuing, is a new market. There is no established market and no industry leader yet. About twenty (20) companies, including Moog and Skyryse, have entered the market and are rushing to become the market leader. Whichever company wins that race will likely win a large portion of the market share just by being the first to market with a viable product. If another party gained access to Moog's flight control software and related data, it would give that party a substantial and unfair competitive advantage as it would save that party literally tens of millions of dollars and several years investing in development and testing that software. Moog has invested approximately five (5) years of research and development into unmanned helicopters and fifteen (15) years in developing the Platform software. As noted, this software takes many years to build, test, and certify. By stealing Moog's source code and other proprietary information underlying Platform and related applications, and crippling Moog's software engineering workforce, Skyryse has jumped to the front of this race to be first to market and has slashed Moog's tires along the way. This race against time underscores the irreparable harm faced by Moog because time cannot be unwound.

144.   Part of what makes Moog unique and competitive in the marketplace is that it can put entire systems for aircraft flight control (*i.e.*, software and hardware) together in-house. Most other competitors can only do one or the other. Moog builds software and hardware components safely through the use of architectural diagrams.

145.   Importantly, there is a high barrier to entry in the flight control software market. Companies that have an established, tested, and proven software and have successfully delivered on contracts before have a huge advantage in securing contracts from the government and other third parties. Platform provides Moog with that competitive advantage. Contracting parties

understand that because of Moog's Platform software, it will be faster and less expensive to tailor its flight control software to a particular aircraft because the substantial foundation has already been built.

146.   On information and belief, other companies would have to pay two to three times what Moog does because Moog has an established flight control operating system software. As a result, Moog wins many of the flight control projects that it bids on.

147.   Kim copied all of Moog's source code, SEPG documents, and other underlying data for Platform and 8 to 9 project-specific applications. This information in the hands of Skyryse removes a large barrier to entry and saves Skyryse tens of millions of dollars and several years of work.

148.   The scope of data copied by Kim is breathtaking in its scope and difficult to comprehend due to its vastness. She essentially copied everything that Moog's flight control software engineering teams had worked on over the past fifteen (15) years. It is impossible to quantify the amount of monetary investment, software engineering hours, and other resources that have gone into developing, testing, and certifying all of these programs and applications. This information is truly priceless and represents the highest level of intelligence and wisdom of Moog's smartest architects of the past 15 to 20 years.

149.   Thousands of employees and millions of hours of work were used in building, testing, and certifying the software and programs copied by Kim.

150.   ██

██

██

██

██

██

██████████   This software application was developed, tested, and certified through the

substantial investment of training, time and money by Moog.

151.   ███

██

██

██   Writing of the code for eRTOS

alone took multiple years. On top of the code building, it takes several additional years to

verify, test, and certify the code under FAA and other international governing body

standards. If a third party wanted to try to build a base flight control operating system

similar to eRTOS, it would take several years to build, test, and certify that software such

that it can be implemented into aircrafts.

152.   One of the notable programs copied by Kim is the commercial program G280,

which Moog built, tested, and certified.   █████████████████████████████

██

██

█████████████████████████████████████

153.   On information and belief, Skyryse is now pursuing flight control systems for

helicopters. The data from the G280 project is directly related to what Skyryse is pursuing and

would be extremely valuable to Skyryse and would save it tremendous time, money, effort, and

resources in having to build these programs from scratch.

154.   It is impossible to precisely quantify the amount of monetary investment, software engineering hours, and other resources that Skyryse stands to save by utilizing Moog's proprietary information and leveraging their former employees' knowledge to deploy that information, but the magnitude is simply massive.

155.   Further, by improperly gaining access to and/or copying Moog's Platform software, a third party could get easier access to perform software upgrades. Currently, only Moog can re-install or service an upgraded equipment or product which uses the Platform software.

156.   Re-programming an airplane computer has several security concerns. A third party would not be able to pull information from an airplane box that has used the Platform software in order to re-program it unless it has access to Moog's software. Moreover, it potentially allows third parties to take over performing work for Moog clients the currently only Moog can perform.

157.   Further, Moog's Platform software has been used for several military programs. Skyryse hired every Moog employee who worked on the eRTOS iteration of the Platform software. It generally takes a new hire one year to obtain sufficient access to work on military projects. Moog is not able to immediately re-allocate new employees to fill the void of its military software developers that left for Skyryse because it takes considerable time to establish required access credentials.

158.   Finally, there are substantial security, goodwill, and reputational issues posed by Kim's copying of Moog's proprietary, confidential, and trade secret software and related data. Under nearly every contract that Moog enters into for flight software development, there is a requirement that Moog notify its customers if certain proprietary or confidential data was copied

or stolen. Moog is now required to notify its customers of the data theft at issue, including the

US Government. This presents a substantial distraction from normal operations and has and will

require Moog to expend resources responding to government inquiries. Moog has never

previously had to notify the US Government of a data theft in connection with its flight control

software.

159.   Moog's required disclosure poses the risk of harm to Moog's reputation and

goodwill in the industry and with customers such as the US Government, which is not

compensable with monetary damages. Data and information security is of paramount concern in

this industry, and especially in performing work for or providing deliverables to the US

Government. Moog has historically been regarded as excellent and trustworthy in terms of data

security and confidentiality.

COUNT I

VIOLATION OF THE DEFEND TRADE SECRETS ACT,
18 U.S.C. § 1836
(Against All Defendants)

160.   Moog incorporates by reference and realleges the allegations contained in

paragraphs 1 through 159 above as if fully set forth herein.

161.   The DTSA forbids threatened and actual misappropriation of trade secrets "if the

trade secret is related to a product or service used in, or intended for use in, interstate or foreign

commerce." 18 U.S.C. § 1836(b)(1) (as amended).

162.   Under the DTSA, "trade secret" means "all forms and types of financial, business,

scientific, technical, economic, or engineering information, including patterns, plans,

compilations, program devices, formulas, designs, prototypes, methods, techniques, processes,

procedures, programs, or codes, whether tangible or intangible, and whether or how stored,

compiled, or memorialized physically, electronically, graphically, photographically, or in writing

if, (A) the owner thereof has taken reasonable measures to keep such information secret, and (B)

the information derives independent economic value, actual or potential, from not being

generally known to, and not being readily ascertainable through proper means by, another person

who can obtain economic value from the disclosure or use of the information." 18 U.S.C.

§ 1839(3) (as amended).

163.   Under the DTSA, "misappropriation" means "(A) acquisition of a trade secret of

another by a person who knows or has reason to know that the trade secret was acquired by

improper means; or (B) disclosure or use of a trade secret of another without express or implied

consent by a person who: (i) used improper means to acquire knowledge of the trade secret; or

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade

secret was: (I) derived from or through a person who had used improper means to acquire the

trade secret; (II) acquired under circumstances giving rise to a duty to maintain the secrecy of the

trade secret or limit the use of the trade secret; or (III) derived from or through a person who

owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the

use of the trade secret; or (iii) before a material change of the position of the person, knew or had

reason to know that (I) the trade secret was a trade secret and (II) knowledge of the trade secret

had been acquired by accident or mistake." 18 U.S.C. § 1839(5) (as amended).

164.   Under the DTSA, "improper means" "(A) includes theft, bribery,

misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage

through electronic or other means; and (B) does not include reverse engineering, independent

derivation, or any other lawful means of acquisition." 18 U.S.C. § 1839(6) (as amended).

165.   Certain confidential and proprietary information of Moog constitutes trade secrets related to a product or service used in, or intended for use in, interstate commerce, including, but not limited to, the underlying source code and SEPG certification process documents for Moog's Platform base software and related project-specific applications.

166.   Moog derives economic value from the fact that its trade secrets and confidential and proprietary information, including the underlying source code and SEPG certification process documents for its Platform base software and related project-specific applications, are not generally known to individuals or entities outside of Moog.

167.   Moog takes reasonable measures to protect the secrecy of such trade secrets and confidential and proprietary information. These measures include, among other things, that: (1) Platform, including all attendant project-specific software, is housed on a secure server at Moog and only certain employees at Moog have access to the software database on a "need to know" basis that must be approved by the lead on the software program; (2) five separate sets of credentials are required to access Moog's software database; (3) Platform software as applied to military projects requires elevated access credentials by the US Government; (4) the Platform software itself is designed to prevent hacking or reverse engineering, and cannot be reverse engineered from an aircraft computer that has used the software; (5) Moog has controlled access into its buildings, and all employees must undergo security screening and background check before being hired; (6) Moog requires its employees to review its employee handbook (which has detailed policies about Moog's confidential and proprietary information, and a prohibition on disclosing or copying such information), acknowledge its receipt, and agree to abide by its policies; (7) Moog has robust written policies regarding its proprietary and trade secret information, and requires its software engineers to complete a training

regarding company trade secrets and other proprietary information to confirm such policies; (8) Moog requires its departing employees to sign an exit form which affirms that they have been granted access to Moog's proprietary information, that they no longer have any access or copies of such materials, and that they will not breach their fiduciary duties to Moog or usurp any corporate opportunity; (9) all Moog flight software source code files are designated as proprietary and confidential and prohibit disclosure; and (10) Moog enters into NDAs with parties where confidential and proprietary information may be disclosed on a limited basis, and in fact entered into multiple NDAs with Skyryse in the past, as explained above.

168.   Both Pilkington and Kim knew they each had a duty to maintain the secrecy of Moog's trade secrets and confidential and proprietary information due, in part, to their fiduciary duty and duty of loyalty to Moog.

169.   Aware of the secrecy and value of Moog's trade secrets and confidential and proprietary information, on information and belief, Skyryse nevertheless coordinated with Pilkington and Kim in efforts to misappropriate such material of and from Moog. Having signed multiple NDAs with Moog in the past, Skyryse was under an additional contractual duty not to violate those NDAs, including by disclosure and use of Skyryse's confidential and proprietary material.

170.   Moreover, having worked with Moog in the past, Skyryse and its C-suite level employees, Messrs. Baptist and Rey were well aware of the value Moog placed on its trade secrets and confidential and proprietary information. Skyryse clearly appreciated how valuable it is – Skyryse originally approached Moog as a business partner because it wanted to use Platform in its own product.

171.   Further, Skyryse is under a duty to not accept any misappropriated trade secrets and confidential and proprietary information, including Moog's trade secrets and confidential and proprietary information, and Skyryse is also under a duty not to disclose or use misappropriated trade secrets and confidential and proprietary information for the purpose of gaining a competitive advantage in the marketplace.

172.   Defendants misappropriated Moog's trade secrets and confidential and proprietary information. On information and belief, under Pilkington's instruction, and in coordination with Skyryse, Kim copied and delivered to Pilkington and Skyryse the data files that she copied from Moog containing Moog's trade secrets and confidential and proprietary information for Skyryse's use in, in connection with, and for the advancement of Skyryse's business. Therefore, Defendants have already willfully and maliciously acquired, disclosed, and used Moog's trade secrets and confidential and proprietary information without consent of any kind for their own financial gain. And Defendants will continue to do so if not enjoined by this Court.

173.   On information and belief, Defendants will continue to disclose and utilize Moog's trade secrets and confidential and proprietary information by using this information to unfairly compete with Moog by improperly using that information in its own development projects and to aid soliciting business for Skyryse.

174.   Indeed, as a result of Defendants' collective actions, Skyryse now has Moog's trade secret, confidential, and proprietary information from theft of over 136,000 files that Skyryse can use and, on information and belief, is using to its competitive advantage.

175.   The actions of Defendants constitute actual or threatened misappropriation under the DTSA.

176.   Moog has suffered damages as a result of Defendants actual and/or threatened breach of the DTSA, including the ongoing loss of employees, harm to its goodwill and reputation, and an unfair reduction in its competitive advantage.

177.   Moog is entitled to actual damages from Defendants, jointly and severally, to exemplary damages pursuant to 18 U.S.C. § 1836(b)(3)(C), and to attorneys' fees pursuant to 18 U.S.C. § 1836(b)(3)(D).

178.   Moog's damages cannot be adequately compensated through remedies at law alone, thereby requiring equitable relief in addition to compensatory relief.

179.   Defendants' actions will continue to cause irreparable harm and damages to Moog and its trade secrets and confidential and proprietary information if not restrained.

COUNT II

MISAPPROPRIATION OF TRADE SECRETS
(Against All Defendants)

180.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 179 above as if fully set forth herein.

181.   In the course of doing business, Moog has acquired and developed highly valuable, trade secrets and confidential and proprietary information.

182.   Certain confidential and proprietary information of Moog constitutes trade secrets related to a product or service used in, or intended for use in, interstate commerce, including, but not limited to, the underlying source code and SEPG certification process documents for its Platform base software and related project-specific applications.

183.   Moog derives economic value from the fact that its trade secrets and confidential and proprietary information, including the underlying source code and SEPG certification

process documents for its Platform base software and related project-specific applications,

are not generally known to individuals or entities outside of Moog.

184.   Moog takes reasonable measures to protect the secrecy of such trade secrets and

confidential and proprietary information. These measures include, among other things, that: (1)

Platform, including all attendant project-specific software, is housed on a secure server at Moog

and only certain employees at Moog have access to the software database on a "need to know"

basis that must be approved by the lead on the software program; (2) five separate sets of

credentials are required to access Moog's software database; (3) Platform software as applied

to military projects requires elevated access credentials by the US Government; (4) the

Platform software itself is designed to prevent hacking or reverse engineering, and cannot

be reverse engineered from an aircraft computer that has used the software; (5) Moog has

controlled access into its buildings, and all employees must undergo security screening and

background check before being hired; (6) Moog requires its employees to review its employee

handbook (which has detailed policies about Moog's confidential and proprietary information,

and a prohibition on disclosing or copying such information), acknowledge its receipt, and agree

to abide by its policies; (7) Moog has robust written policies regarding its proprietary and

trade secret information, and requires its software engineers to complete a training

regarding company trade secrets and other proprietary information to confirm such

policies; (8) Moog requires its departing employees to sign an exit form which affirms that

they have been granted access to Moog's proprietary information, that they no longer have

any access or copies of such materials, and that they will not breach their fiduciary duties

to Moog or usurp any corporate opportunity; (9) all Moog flight software source code files

are designated as proprietary and confidential and prohibit disclosure; and (10) Moog

enters into NDAs with parties where confidential and proprietary information may be disclosed on a limited basis, and in fact entered into multiple NDAs with Skyryse in the past, as explained above.

185.   Platform cannot be copied off of any of the aircraft in which it is deployed, nor can any of Moog's clients access the source code through any other mechanism in the course of using Platform. In other words, no one other than Moog employees can access, download, review and modify Platform.

186.   Both Pilkington and Kim knew they each had a duty to maintain the secrecy of Moog's trade secrets and confidential and proprietary information due, in part, to their fiduciary duty and duty of loyalty to Moog.

187.   Aware of the secrecy and value of Moog's trade secrets and confidential and proprietary information, on information and belief, Skyryse nevertheless coordinated with Pilkington and Kim in efforts to misappropriate such material of and from Moog. Having signed multiple NDAs with Moog in the past, Skyryse was under an additional contractual duty not to violate those NDAs, including by disclosure and use of Skyryse's confidential and proprietary material.

188.   Further, Skyryse is under a duty to not accept any misappropriated trade secrets and confidential and proprietary information, including Moog's trade secrets and confidential and proprietary information, and Skyryse is also under a duty not to disclose or use misappropriated trade secrets and confidential and proprietary information for the purpose of gaining a competitive advantage in the marketplace.

189.   Defendants misappropriated Moog's trade secrets and confidential and proprietary information. On information and belief, under Pilkington's instruction, and in

coordination with Skyryse, Kim copied and delivered to Pilkington and Skyryse the data

files that she copied from Moog containing Moog's trade secrets and confidential and

proprietary information for Skyryse's use in, in connection with, and for the advancement

of Skyryse's business. Therefore, Defendants have already willfully and maliciously acquired,

disclosed, and used Moog's trade secrets and confidential and proprietary information without

consent of any kind for their own financial gain. And Defendants will continue to do so if not

enjoined by this Court.

190.   On information and belief, Defendants will continue to disclose and utilize

Moog's trade secrets and confidential and proprietary information by using this information to

unfairly compete with Moog by improperly using that information in its own development

projects and to aid soliciting business for Skyryse.

191.   Indeed, as a result of Defendants' collective actions, Skyryse now has over

Moog's trade secret, confidential, and proprietary information from theft of over 136,000 files

that Skyryse can use and, on information and belief, is using to its competitive advantage.

192.   The misappropriation by all Defendants has directly and proximately caused

Moog to suffer great damage and injury, and Moog will continue to suffer damage by the

continued acts of Defendants.

COUNT III

BREACH OF FIDUCIARY DUTY AND DUTY OF LOYALTY
(Against Pilkington and Kim)

193.   Moog incorporates by reference and realleges the allegations contained in

paragraphs 1 through 192 above as if fully set forth herein.

194.   By virtue of Pilkington's and Kim's employment relationship with Moog,

including assignment to sensitive programs requiring additional vetting and commitment to the

protection of such information from misuse, Moog reposed trust and confidence in each of Pilkington and Kim to provide services and perform their duties, and to refrain from acting in any manner contrary to Moog's interests.

195.   Pilkington and Kim each undertook such trust and confidence.

196.   By reason of the foregoing, Pilkington and Kim each owed Moog a fiduciary duty and duty of loyalty to act in good faith and in Moog's best interest, which includes a duty not to disclose or use the employer's proprietary or confidential information for the purpose of competing with their employer or for his or her own personal gain. These duties were confirmed and agreed in writing in at least Kim's Exit Form, which she signed on December 17, 2021.

197.   Such fiduciary duty and duty of loyalty owed by Pilkington and Kim to Moog existed throughout their respective employments with Moog and survived the termination of that employment.

198.   Pilkington and Kim breached their fiduciary duty and duty of loyalty to Moog by engaging in the wrongful activity as described herein, including but not limited to, the misappropriation of Moog's trade secrets and confidential and proprietary information for their benefit and the benefit of Skyryse, a competitor of Moog, and by scheming to solicit away employees of Moog while still employed by Moog.

199.   Pilkington's and Kim's actions were and are willful and malicious and without legal justification or excuse.

200.   Pilkington's and Kim's breach of their fiduciary duty of loyalty has and will continue to directly and proximately cause substantial damage to Moog and its business, including damage to its reputation.

201.   Pilkington's and Kim's breach of their fiduciary duty of loyalty has directly and proximately caused Moog to suffer great damage and injury, and Moog will continue to suffer damage and injury by the continued acts of Pilkington and Kim.

<div align="center">

COUNT IV

AIDING AND ABETTING BREACH OF FIDUCIARY DUTY
(Against Pilkington)

</div>

202.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 201 above as if fully set forth herein.

203.   Pilkington aided and abetted Kim's breach of fiduciary duty by collaborating with her to misappropriate Moog's trade secrets and confidential and proprietary information, and by contributing to and encouraging her tortious activity.

204.   On information and belief, Pilkington had actual knowledge of Kim's breach of fiduciary duty, as he knew that she was providing him and Skyryse with Moog's proprietary and confidential files in furtherance of her own self-interest and in furtherance of the interests of Pilkington and Skyryse. Pilkington provided substantial assistance by collaborating with Kim to misappropriate what they knew to be Moog's confidential, proprietary, and trade secret information. Indeed, upon information and belief, Pilkington directed Kim to use Pilkington's file path in copying Moog's data. Pilkington aided and abetted Kim's breach of fiduciary duty intentionally and without justification.

205.   The participation of Pilkington in the breach of Kim's fiduciary duties has and will directly and proximately cause substantial damage to Moog and its business, including damage to its reputation.

206.   The participation of Pilkington in the breach of Kim's fiduciary duties has

directly and proximately caused Moog to suffer great damage and injury, and Moog will

continue to suffer damage by the continued acts of Pilkington.

COUNT V

UNFAIR COMPETITION
(Against Skyryse)

207.   Moog incorporates by reference and realleges the allegations contained in

paragraphs 1 through 206 above as if fully set forth herein.

208.   Upon information and belief, Skyryse has, in bad faith, employed unfair

means, including but not limited to inducing Pilkington and Kim to: violate their duties of

loyalty to Moog; lure away key software development employees from Moog; and,

misappropriate Moog's trade secret, confidential, and proprietary information, as part of a

deliberate and malicious strategy to harm Moog's business and unfairly trade on Moog's

investments of time and money in software and employees.

209.   To date, Skyryse has successfully raided 20 Moog employees, including

high-level Moog officers, senior level engineers, coding engineers, and testers, and has

reached out to many software engineers at Moog who worked on the Platform software or

related project-specific applications in the United States, specifically targeting Moog's Los

Angeles-area office.

210.   Replacing these lost employees has massively slowed work production due to

the elevated access credentials needed to support the Sensitive Government Programs.

211.   Upon information and belief, Skyryse has raided these employees as part of

its scheme to gain access to confidential, proprietary trade secret information, including but

not limited to its Platform base software and related project-specific applications. Upon

information and belief, in concert with its new employees Pilkington and Kim, Skyryse has improperly and wrongfully acquired this information.

212.   Skyryse misappropriated Moog's trade secrets and confidential and proprietary information on its own and in coordination with Pilkington and Kim.

213.   Upon information and belief, Skyryse has used and continues to use Moog's trade secrets and confidential and proprietary information to gain a competitive advantage over Moog (and other competitors) in the flight control software market.

214.   Skyryse has no legitimate business justification for its actions and such actions were done in bad faith and with the intent to harm Moog.

215.   Skyryse's unfair competition has and will directly and proximately cause substantial damage to Moog and its business, including the loss of market share and prospective customers, loss of its trade secrets and confidential and proprietary information, and damage to its reputation.

216.   Skyryse's acts of unfair competition have and will directly and proximately cause Moog to suffer great damage and injury, and Moog will continue to suffer damage by the continued acts of Skyryse.

COUNT VI

CONSPIRACY
(Against All Defendants)

217.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 216 above as if fully set forth herein.

218.   As alleged above, Defendants committed the underlying tort of misappropriation of Moog's trade secrets.

219.   On information and belief, each of the Defendants reached an agreement to commit the above alleged tort. This agreement is indicated by their collaboration and cooperation to use Moog's trade secret, confidential and proprietary information in and for Skyryse's business.

220.   On information and belief, each of the Defendants committed an act in furtherance of the agreement to commit the above alleged torts, as indicated by their collaboration and cooperation to use Moog's trade secret, confidential and proprietary information in and for Skyryse's business. Gonzalo Rey was also involved in, and a key orchestrator of, the conspiracy alleged herein. Rey, an executive at Moog who pioneered the development of its flight control software, was the first Moog employee to join Skyryse. He is now a high-level executive at Skyryse pursuing the development of a competing flight control software, and he has been the lead individual involved in Skyryse's targeted solicitation of Moog's software engineers.

221.   Defendants' conspiracy to commit the above alleged tort has and will directly and proximately cause substantial damage to Moog and its business, including the loss of market share and prospective customers, loss of its trade secrets and confidential and proprietary information, and damage to its reputation.

222.   Defendants' conspiracy to commit the above alleged tort has and will directly and proximately cause Moog to suffer great damage and injury, and Moog will continue to suffer damage by the continued acts of Defendants.

///

///

///

COUNT VII

BREACH OF CONTRACT
(Against Skyryse)

223.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 222 above as if fully set forth herein.

224.   As explained above, on October 24, 2018, Moog and Skyryse entered into the 2018 NDA, and, on March 15, 2019, Moog and Skyryse entered into the 2019 NDA.

225.   Section 2 of the 2018 and 2019 NDAs provides: "Neither Party shall disclose, in whole or in part, by any means whatsoever, any Proprietary Information provided by the disclosing Party to any third party without the express prior written consent of the disclosing Party. The receiving Party shall not alter, modify, decompile, disassemble, reverse engineer, translate or create derivative works from the disclosing Party's Proprietary Information. The receiving Party shall use Proprietary Information of the disclosing Party only for the limited purpose described above and not for any other purpose."

226.   Section 3 of the 2018 and 2019 NDAs provides: "Each Party shall utilize the same degree of care to preserve and protect the other Party's Proprietary Information from disclosure, and otherwise limit access, as it uses to protect its own Proprietary Information, which degree of care will not be less than reasonable care."

227.   Section 5 of the NDAs confirms the effective term for both agreements is ten years for the execution date.

228.   Section 8 of the NDAs provides: "A breach of any of the terms of this Agreement will result in irreparable and continuing damage for which there may be no adequate remedy at law and the non-breaching Party shall be entitled to seek injunctive relief, without the necessity of posting a bond, and such other relief, including monetary damages, if appropriate, against the

breaching Party am/or any other person or entity liable for the unauthorized or wrongful use or disclosure of Proprietary Information received hereunder."

229.   In breach of the 2018 NDA and 2019 NDA, upon information and belief, Skyryse used information gained from Moog regarding its flight control software for purposes beyond the scope of the limited purpose of the Parties' business engagement in Phase 1 under the SOW including to: 1) develop its own flight control systems and software; and 2) raid and solicit Moog's key software engineering personnel who have most knowledge of Moog's flight control software. Upon information and belief, Skyryse attempted to or in fact did reverse engineer certain components of Moog's flight control systems in an effort to develop a competing flight control system, which is expressly prohibited under the 2018 and 2019 NDAs. Upon information and belief, Skyryse used confidential information provided by Moog under the 2018 and 2019 NDAs regarding Moog's software engineering staff and technology to engage in targeted hiring and data theft practices a few years later.

230.   Skyryse's breaches of the 2018 NDA and 2019 NDA directly and proximately caused and continue to cause Moog to suffer great damage and injury, and Moog will continue to suffer damage as a result of Skyryse's ongoing breaches of the 2018 NDA and 2019 NDA.

COUNT VIII

BREACH OF CONTRACT
(Against Pilkington and Kim)

231.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 230 above as if fully set forth herein.

232.   Pilkington acknowledged its receipt of the Employee Handbook and agreed to abide by its policies on July 30, 2012. Kim acknowledged its receipt and agreed to abide by its policies on January 21, 2013.

233.   On Page 58, the Employee Handbook provides: "Unless acting in the proper performance of your duties, or required by law, you must not disclose to any person or body, including work colleagues, or use any confidential information that you obtain during the course of your employment. These restrictions will continue after your employment has been terminated."

234.   On Page 59, the Employee Handbook provides: "Confidential information belonging to the company will remain the property of the company and you must not retain any copies of this information . . . Any breach of confidentiality, including the imparting of information to other employees, except on a ''need to know' basis, will be considered grounds for summary dismissal and breach of contract for which damages may be claimed."

235.   Pilkington and Kim breached the terms of Moog's Employee Handbook by engaging in the wrongful activity as described herein, including but not limited to, the misappropriation of Moog's trade secrets and confidential and proprietary information for their benefit and the benefit of Skyryse, a competitor of Moog, and by scheming to solicit away employees of Moog while still employed by Moog.

236.   Further, Kim signed the Exit Form on her last date of employment at Moog on December 17, 2021.

237.   In the Exit Form, Kim agreed that she that she had returned all Moog "TRADE SECRET/COMPANY CONFIDENTIAL INFO." The Exit Form also provides, among other

things: 1) Kim "owes a fiduciary duty to Moog to not usurp any such corporate opportunity for [her] own benefit"; and 2) Kim affirms that she does "not maintain access to, or have possession of, any tangible or digital record of Moog IP-whether in hard copy or digital form—on any device, cloud, or digital storage facilities."

238.   Kim breached her obligations under the Exit Form because she: 1) copied over 136,000 files of confidential and proprietary Moog data and kept it with her after her employment ended; 2) deleted the Moog data she copied on the external hard drive she used; and breached her fiduciary duties to Moog by usurping Moog's corporate opportunities to the benefit of herself, Pilkington, and Skyryse.

239.   Pilkington's and Kim's respective breaches of said agreements directly and proximately caused and continue to cause Moog to suffer great damage and injury, and Moog will continue to suffer damage as a result of Pilkington's and Kim's respective ongoing breaches of those agreements.

COUNT IX

TORTIOUS INTERFERENCE WITH
PROSPECTIVE ECONOMIC ADVANTAGE
(Against All Defendants)

240.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 239 above as if fully set forth herein.

241.   Moog had a reasonable expectation of entering into a valid business relationship with the US Government with regard to development of project-specific software applications for military use, which sit on top of the Platform flight control operating system, and specifically, the "eRTOS" base software designed. Some of Moog's project-specific software applications for military use which sit on top of the eRTOS base are titled "Bell

V280," "TERN," "X47B," Sensitive Government Program 1, and Sensitive Government

Program 2, which Moog has developed at its own great cost and expense.

242.   The Platform software as applied to military projects are extremely

confidential, and require elevated access credentials to support sensitive US Government

programs. Only a limited number of certain individuals at Moog have the elevated access

credentials, which takes around a year to obtain. Moog expected to be able to utilize its

employees that had gained such elevated access credentials for execution of the military

projects.

243.   Additionally, Moog expected to be able to keep sensitive certain proprietary

and confidential information files (including coding, testing, and certification files) related to

the particular military programs and in compliance with the US Government's requirements..

244.   However, at the instruction of Pilkington, and in coordination with Skyryse, Kim

copied nearly all of the files (including coding, testing, and certification files) related to Sensitive

Government Programs 1 and 2. Also, at the instruction of Pilkington, and in coordination with

Skyryse, Kim copied nearly all of the files (including coding, testing, and certification files)

related to the eRTOS Platform flight control software. Sensitive Government Programs 1 and 2

and eRTOS programs are just a few of the many programs that Kim copied in their entirety or

near entirety, at the instruction of Pilkington, and in coordination with Skyryse.

245.   Defendants had knowledge of Moog's expectancy.

246.   Nevertheless, Defendants engaged in a coordinated raid of Moog's employees,

including the hiring away of several key employees with the access necessary for execution of

the military projects, and engaged in misappropriation of proprietary and confidential

information files related to the particular military programs. For example, every software engineer who worked on eRTOS was hired by Skyryse.

247.   In doing so, Defendants acted for a wrongful purpose and used dishonest, unfair, and improper means.

248.   Additionally, Defendants' tortious actions have interfered with and injured Moog's ongoing business relationship with the US Government. As described above, under every contract that Moog enters into for flight software development, there is a requirement that Moog notify the US Government if certain proprietary or confidential data was copied or stolen. Moog is now required to notify customers, including the US Government, of the data theft at issue. Moog has never experienced any prior instance where it had to notify the US Government of a data theft involving its flight control software. Upon information and belief, Moog's reputation and goodwill with the United States has been damaged, as the US Government is extremely concerned with data and information security. Upon information and belief, Moog's ability to obtain future contracts with the US Government could be impaired or delayed as a result of Kim's actions if not promptly addressed and remedied.

249.   Defendants' acts of tortious interference with Moog's prospective economic relations have and will directly and proximately cause damage to Moog and its business, including the loss of market share and prospective customers, loss of its trade secrets and confidential and proprietary information, and damage to its reputation.

250.   Defendants' acts of tortious interference with Moog's prospective economic relations have and will directly and proximately cause Moog to suffer damage and injury, Moog will continue to suffer damage by the continued acts of Defendants.

COUNT X

UNJUST ENRICHMENT
(Against All Defendants)

251.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 250 above as if fully set forth herein.

252.   Defendants have unjustly received and retained the benefits of the efforts and investments of Moog to the detriment of Moog.

253.   Defendants have unjustly and improperly utilized to their benefit the Moog's effort and investment in a host of employees raided by Defendants and in confidential and proprietary information developed by Moog, to the benefit of Skyryse's business and the advantage of Pilkington and Kim.

254.   Defendants have been unjustly enriched, and it is against equity and good conscience to permit Defendants to retain the benefits of the efforts and investments of Moog.

255.   Moog has no adequate remedy at law.

COUNT XI

IMPOSITION OF CONSTRUCTIVE TRUST
(Against All Defendants)

256.   Moog incorporates by reference and realleges the allegations contained in paragraphs 1 through 255 above as if fully set forth herein.

257.   At all times during their employment at Moog, and continuing after their employment, Pilkington and Kim owed fiduciary duties of loyalty and care to Moog. These duties, including obligations not to misappropriate or disclose Moog's proprietary and trade secret information, were further confirmed in Moog's trade secret trainings, the Exit Form, Moog's designations on its source code documents, and elsewhere.

258.   During their employment, Pilkington and Kim promised not to misappropriate, misuse, or otherwise disclose Moog's confidential, proprietary, and trade secret information, and to not usurp a corporate opportunity of Moog.

259.   In reliance on these promises, Moog granted access credentials to Pilkington and Kim to Moog's most confidential, proprietary, and trade secret information, including but not limited to the source code for Platform and project-specific applications, as well as the SEPG checklists and related documents. Pilkington and Kim knew that they were only allowed to access these programs for legitimate business purposes of Moog. As described above, Pilkington and Kim used this position of trust and confidence to orchestrate a scheme to copy and steal over 136,000 files of Moog's data shortly after Pilkington left Moog and a few weeks before Kim did.

260.   Similarly, Moog and Skyryse entered into a confidential relationship as evidenced by the 2018 and 2019 NDAs, which expressly prohibited use of confidential information disclosed thereunder beyond the scope of the Parties' contemplated business arrangement at the time.

261.   Skyryse therefore promised not to use Moog's confidential and trade secret information for its own gain beyond the scope of the NDAs. In reliance on that promise, Moog provided considerable confidential information under the NDAs, including certain information related to its flight control systems and software functionalities.

262.   As alleged above, Skyryse used the confidential information that Moog provided under the NDAs in an improper manner, including to develop its own competing flight control systems and software, and to raid and solicit Moog's most knowledgeable employees regarding its flight control software.

263.   Defendants, and each of them, have been unjustly enriched by the confidential, proprietary, and trade secret information that they have improperly used and stolen from Moog. Upon information and belief, Defendants are using the misappropriated Moog data to develop its own competing flight control software to the direct harm of Moog.

264.   Moog has no remedy at law to address this misconduct. Defendants are in possession of a large volume of Moog data and information of which they have no right to possess. It is just and equitable that this Court impose a constructive trust to attach on all of Moog's confidential information and data that Defendants, and each of them, improperly took and from the time it entered their possession.

WHEREFORE, Moog demands judgment against Defendants as follows:

(1)   For a temporary, preliminary and permanent injunction enjoining Defendants and their agents, servants, employees, officers, attorneys, successors, licensees, partners, and assigns, and all other persons acting in concert with them from:

> (a) directly or indirectly using, accessing, disclosing, copying, or transmitting, for any purpose, any non-public information, documents, records, files, or data in any Defendant's possession, custody, or control (i) of, from, or belonging to Moog, (ii) provided, offered, transmitted, or conveyed to any Defendant by any current or former Moog employee, and/or (iii) copied or taken from Moog's computers, servers, databases, networks, or systems, including without limitation any and all information, documents, files, or data copied or downloaded by Kim and/or Pilkington from Moog's computers, servers, databases, or systems, regardless of the medium on which such materials were copied, transferred, or stored;

> (b) directly or indirectly soliciting, influencing, inducing, recruiting or causing any Moog employee in Moog's aircraft flight control business to terminate his or her employment for the purpose of joining, associating or becoming employed with Skyryse;

> (c) continuing to possess or use Moog's confidential, proprietary, and/or and trade secret information;

(d) preserving and turning over all evidence of any non-public information, documents, records, files, or data in any Defendant's possession, custody, or control belonging to Moog; and

(e) such other relief as the Court may deem appropriate as against Defendants;

(2)   For an award of Moog's actual damages and lost profits it has sustained as a result of Defendants' unlawful acts of misappropriation of Moog's trade secrets and confidential information, and to recover from Defendants' the gains, profits, and advantages Defendants have obtained as a result of the wrongful conduct alleged herein, in an amount to be determined at trial;

(3)   For an order awarding Moog its attorneys' fees under the Defend Trade Secrets Act 18 U.S.C. § 1836(b)(3)(D);

(4)   For an imposition of a constructive trust on the information and data that Defendants wrongfully took from Moog and held by Defendants (and any profits derived therefrom), and order that such information be held for Moog's benefit and transferred in full to Moog;

(5)   For an order awarding Moog exemplary damages in an amount twice the amount of actual damages awarded, for willful and malicious misappropriation under the Defend Trade Secrets Act pursuant to 18 U.S.C. § 1836(b)(3)(D);

(6)   For an order awarding Moog all costs, litigation expenses, and actual, reasonable attorneys' fees pursuant to the breached contracts;

(7)   For an award of compensatory damages against Defendants in favor of Moog;

(8)   For an award of punitive damages against Defendants and in favor of Moog;

(9)   For an order that Moog recover its costs from Defendants;

(10)   For prejudgment and postjudgment interest at the New York statutory rate of 9% per annum; and

(11)   For such other and further relief as the Court deems just and proper.

<div align="center">

DEMAND FOR JURY TRIAL

</div>

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Moog demands a

trial by jury of all issues so triable.

Dated: New York, New York
        March 7, 2022

SHEPPARD, MULLIN, RICHTER & HAMPTON LLP
Attorneys for Plaintiff Moog Inc.

By:＿＿＿s/Rena Andoh＿＿＿＿＿
      Rena Andoh
      Travis J. Anderson (*pro hac vice* forthcoming)
      Tyler E. Baker (*pro hac vice* forthcoming)
      Kazim A. Naqvi (*pro hac vice* forthcoming)
30 Rockefeller Plaza
New York, New York 10112
Telephone: (212) 653-8700'

and

HODGSON RUSS LLP

By:＿＿＿s/Robert Fluskey＿＿＿＿
      Robert J. Fluskey, Jr.
      Melissa N. Subjeck
      Pauline T. Muto
The Guaranty Building
140 Pearl Street, Suite 100
Buffalo, New York 14202
(716) 856-4000